AMENDMENTS TO THE CLAIMS

A detailed listing of all claims that are, or were, in the present application, irrespcctive of whether the claim(s) rcmains under examination in the application are presented below. The claims are presented in ascending order and each includes one status identifier. Those claims not cancelled or withdrawn but amended by the current amendment utilize the following notations for amendment: 1. deleted matter is shown by strikethrough for six or more characters and double brackets for five or less characters; and 2. added matter is shown by underlining.

1-24. (Canceled).

25. (Currently Amended) A method for initiating a private secure connection between at least one client and a remote server interconnected by a public network for transmission of enciphered communications ~~over a public network using a layered communications protocol characterized by a protocol stack~~, the method comprising the steps of:

equipping the rcmote server with at lcast onc secure processor configured for running at least one secure server process for independently initiating and maintaining a private secure connection with the at least one client;

communicatively coupling ~~providing~~ a first secure receipt pre-processor and a response manager ~~equipped to run a first process to enable communications with~~ to the at least one client via the public network and to the remote server via a protocol stack associated with a first layered communication protocol,~~;~~

~~communicatively coupling a first response manager to the first secure receipt pre-~~

~~processor;~~

~~placing the remote server in data communications with the first secure receipt pre-processor and the first response manager, the data communications being intermediated by the protocol stack and~~ the remote server being configured with an operating system operative to selectively direct ~~a first~~ the at least one secure server process;

storing at least one user supplied configuration option expressing at least one secure server process capability supporting the initiating and maintaining of the private secure connection with the at least one client;

receiving at the first secure receipt pre-processor, mediated by an interface compatible with the first layered communication protocol, a first client ~~request~~ communication originating at the at least one client and transmitted over the public network using the first layered communication protocol , the first client communication expressing at least one client capability supporting the ~~initiation~~ initiating of the private secure connection with the remote server;

storing the first client communication after retaining a pointer to the first client communication;

responsivc to the receipt of the first client ~~request~~ communication, generating at the first secure receipt pre-processor, ~~under control~~ independent of the first secure server process, a first client-related identification object based on the first client communication;

gcnerating a first client-related data-object embodying the pointer to the first client communication, a time-stamp obtained from the operating system and the first client-related identification object;

hashing the identification object using a hashing algorithm to create a first hash index;

storing the first client-related data-object indexed by the first hash index after associating a unique session identifier to the first-client-related data object;

comparing thc at least one user supplied configuration option with the first client-related data object to generate a portion of a complete first server ~~response~~ communication to the client that is consistent with the at least one capability expressed in the first client ~~request~~ communication;

based upon the portion of the complete first server response and the layered communications protocol, generating at the response manager and communicating to the at least one client the complete first server communication ~~response~~ responsive to thc first client ~~request~~ communication and expressing at least one server capability for supporting the initiation of the private securc connection with the at least first client;

responsive to the receipt of the complete first server communication ~~response~~ at the at least one client, receiving at the first secure receipt pre-processor a first client reply, mediated by the interface compatible with the first layered communication protocol, containing a pre-master secret transmitted from the client, the pre-master secret being based at least in part upon the complete first server communication ~~response~~ communicated to the at least one client by the response manager;

~~responsive to the first client reply, creating~~ generating at the first secure receipt pre-processor, ~~under control~~ independent of the first secure server process, a second client-related identification object based on the first client reply;

retrieving the first client-related data-object embodying the first client-related identification object matching the second clicnt-rclatcd idcntification object;

generating a first remote server response under direction of the first secure server process by using the first client-related data-object ~~request~~ forwarded to the remote server through the intermediation of the protocol stack;

communicating the first remote server response to the response manager, through the intermediation of the protocol stack ~~to cause the response manager to~~ ~~communicate the client reply, through the intermediation of the protocol stack, to the remote server;~~ at the response manager, creating a first server-related search object based on the first server response;

under direction of the first secure server process, generating a session key using the pre-master secret in the first client reply; and

encrypting subsequent communications, ~~intermediated by the protocol stack,~~ between the remote server and the at least one client over the public network using the session key.

26. (Currently Amended) A method for initiating a private secure session for secured data communications over an unsecured network, the method comprising:

providing a server running under an operating system that controls at least a first process and a second process, the server including a secure receipt pre-processor, a response manager and a secure processor communicatively coupled to each other, wherein the secure receipt pre-processor and optionally the response manager are operationally directed by the first process and the secure processor is operationally directed by the second process;

receiving a [[first]] client [[hello]] communication from a client at the secure receipt pre-processor;

classifying the client [[hello]] communication ~~including~~ ~~at least~~ into one of a client hello having a first expression indicative of initiating the private secure session with the secure processor, a client reply having a pre-master secret created responsive to a server hello, and an encrypted client communication;

if the received client communication is the client hello and the client hello is missing a secure session identifier, buffering the [[first]] client hello at the secure receipt pre-processor after generating and assigning a secure session identifier to the [[first]] client hello, and saving the secure session identifier;

responsive to the [[first]] client hello, generating and forwarding to the client a [[first]] server hello cooperatively between the secure receipt pre-processor and the response manager independent of the second process, the server hello including at least one second expression to enable the client to initiate the private secure session;

if the received client communication is the client hello and the client hello includes the secure session identifier, locating the secure session identifier and examining a timestamp associated with the secure session identifier;

if the timestamp associated with secure session identified is unacceptable, generating and forwarding to the client the server hello cooperatively between the secure receipt pre-processor and the response manager independent of the second process, the server hello including the at least one second expression to enable the client to initiate the private secure session;

if the timestamp associated with secure session identified is acceptable, substituting the secure session identifier by a sever session identifier, sending the client hello to the secure server, receiving and examining a secure server reply;

upon detecting a secure server reply that is a server hello, saving the server session identification and the timestamp before forwarding the server hello to the client, otherwise forwarding the secure server reply to the client;

upon receiving ~~a first~~ the client reply at the secure receipt pre-processor responsive to the first client hello, wherein the [[first]] client reply [[being]] is in a first ciphertext form and including the ~~at least one~~ pre-master secret based at least in part on the at least one second expression[[;]], ~~responsive to receiving the first client reply~~, forwarding the [[first]] client hello~~,~~ ~~that matches client reply~~ that corresponds to the ~~buffered dial hello~~ client reply received at the secure receipt pre-processor[[,]] to the secure processor;

~~to cause the secure processor to~~ ~~register~~ assigning the ~~secure~~ server session identifier associated with the first client hello [[with]] to the private secure session;

using the pre-master secret in the [[first]] client reply to generate a session key at the secure server; and

using the session key to process encrypted client communications at the secure server and for encrypting communications ~~between~~ before forwarding to the client ~~and the secure server using the session key~~.

Please add new claims 27-29 as follows:

27. (New) The method of claim 25 wherein the step of generating the first complete server response to the client further includes the steps of:

choosing a lesser of a protocol version contained in the first client communication and a protocol version in the at least one user supplied configuration option if the first client communication contains a protocol version;

choosing a first compression method indicated in a list of compression methods contained in the first client communication that is also in a list of compression methods in the at least one configuration options if the first client communication contains a list of compression methods;

examining a "request client authentication" option stored in the at least one user supplied configuration option and upon the "request client authentication" option being true, constructing a client authentication request; and

examining a "provide server authentication" option stored in the at least one user supplied configuration option, and upon the "provide server authentication" option being true, examining a chosen cipher and using the chosen cipher to choose a server authentication from a ccrtificate storage.

28. (New) The method of claim 25 wherein the hashing algorithm comprises an algorithm selected from the set consisting of one of: a Rivest Shamir Adleman (RAS), a Message-Digest algorithm 5 (MD5) and a Secure Hash Algorithm (SHA).

29. (New) The method of claim 25 wherein the layered communication protocol is the Transfer Control Protocol (TCP).